(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（A）**　(11)特許出願公開番号

特開平4－321143

(43)公開日　平成４年(1992)11月11日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/00	５３７　Ａ	8944－5B		

審査請求　有　　請求項の数54(全 17 頁)

(21)出願番号　特願平4－17406

(22)出願日　平成４年(1992)２月３日

(31)優先権主張番号　６７８５７２

(32)優先日　1991年３月28日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　リチヤード、デール、ホフマン
アメリカ合衆国テキサス州、オースチン、ベン、クレンシヨー、ウエイ、1529

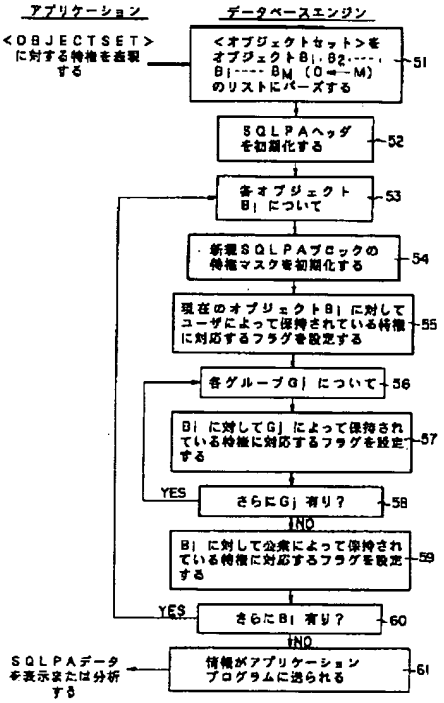
(74)代理人　弁理士　頓宮　孝一　（外５名）

(54)【発明の名称】　データベースオブジエクトのユーザアクセス特権を判定するための汎用的方法および製品ならびにその方法を実施するためのコンピユータシステム

(57)【要約】

【目的】　データベースのオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための方法、コンピュータシステムおよび製品を提供する。

【構成】　（ａ）所与のユーザがアクセス特権を有するオブジェクトの判定を要求する段階と、（ｂ）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定する段階と、（ｃ）そのユーザが間接アクセス特権を有するオブジェクトを自動的に判定する段階とを含む。この最後の段階（ｃ）は、（１）そのユーザが属する全部のアクセスグループを自動的に判定する段階と、（２）段階（１）で判定されたそれらのアクセスグループがアクセス特権を有するオブジェクトを自動的に判定する段階によって遂行される。



1

【特許請求の範囲】

【請求項1】データベースのオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための方法であって、（a）所与のユーザがアクセス特権を有するオブジェクトの判定を要求する段階と、（b）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定する段階と、（c）そのユーザが間接アクセス特権を有するオブジェクトを、（1）そのユーザが属する全部のアクセスグループを自動的に判定する段階と、（2）段階（1）で判定された前記アクセスグループがアクセス特権を有するオブジェクトを自動的に判定する段階によって、自動的に判定する段階とを含むことを特徴とする方法。

【請求項2】請求項1記載の方法であって、段階（c）がさらに、公衆がアクセス特権を有するオブジェクトを自動的に判定する段階を含むことを特徴とする方法。

【請求項3】請求項1記載の方法であって、さらに、前記ユーザがアクセス特権を有するオブジェクトを表示させる段階を含むことを特徴とする方法。

【請求項4】請求項1記載の方法であって、前記要求段階が、（1）アクセス特権を記述するためにコマンドを発行する段階と、（2）記述されるオブジェクトの型を述べる段階と、（3）記述されるオブジェクトの名称を述べる段階と、（4）アクセス特権情報を受け取る制御ブロックの名称を述べる段階とを含むことを特徴とする方法。

【請求項5】請求項1記載の方法であって、さらに、（d）前記ユーザがアクセス特権を有する各オブジェクトへのアクセスの型を判定する段階と、（e）各自のオブジェクトとともに前記アクセスの型を表示させる段階とを含むことを特徴とする方法。

【請求項6】請求項1記載の方法であって、前記方法が、多数のデータベース製品によって使用するための非手続きコンピュータ言語で実施されることを特徴とする方法。

【請求項7】請求項1記載の方法であって、前記方法が、特定のデータベース製品によって使用するためのアプリケーションプログラム言語で実施されることを特徴とする方法。

【請求項8】請求項1記載の方法であって、前記オブジェクトが、コレクション、索引、パッケージおよびテーブルを含むことを特徴とする方法。

【請求項9】請求項1記載の方法であって、前記オブジェクト型が、コレクション、索引、パッケージおよびテーブルの1以上を含むことを特徴とする方法。

【請求項10】データベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための方法であって、（a）そのユーザがその所与のオブジェクトに対してアクセス特権を有するかの判定を要求する段階と、（b）そのユーザ

2

がそのオブジェクトに対して直接アクセス特権を有するかを自動的に判定する段階と、（c）そのユーザがそのオブジェクトに対して間接アクセス特権を有するかを、（1）そのユーザが属する全部のアクセスグループを自動的に判定する段階と、（2）段階（1）で判定されたアクセスグループの1以上がそのオブジェクトに対してアクセス特権を有するかを自動的に判定する段階によって、自動的に判定する段階とを含むことを特徴とする方法。

【請求項11】請求項10記載の方法であって、段階（c）がさらに、公衆がそのオブジェクトに対してアクセス特権を有するかを自動的に判定する段階を含むことを特徴とする方法。

【請求項12】請求項10記載の方法であって、さらに、それを通じてユーザがそのオブジェクトに対してアクセス特権を有する各アクセスグループまたは複数のアクセスグループを表示させる段階を含むことを特徴とする方法。

【請求項13】請求項10記載の方法であって、前記要求段階が、（1）アクセス特権を記述するためにコマンドを発行する段階と、（2）その所与のオブジェクトの型を述べる段階と、（3）そのオブジェクトの名称を述べる段階と、（4）アクセス特権情報を受け取る制御ブロックの名称を述べる段階とを含むことを特徴とする方法。

【請求項14】請求項10記載の方法であって、さらに、（d）ユーザがそのオブジェクトに対して有するアクセス特権の型を判定する段階と、（e）前記アクセスの型を表示させる段階とを含むことを特徴とする方法。

【請求項15】請求項10記載の方法であって、さらに、（f）そのオブジェクトのアクセス特権が他のユーザに拡張できるかどうかを判定する段階と、（g）そのオブジェクトのアクセス特権が他のユーザに拡張できるかどうかを表示させる段階とを含むことを特徴とする方法。

【請求項16】請求項10記載の方法であって、前記方法が、多数のデータベース製品によって使用するための非手続きコンピュータ言語で実施されることを特徴とする方法。

【請求項17】請求項10記載の方法であって、前記方法が、特定のデータベース製品によって使用するためのアプリケーションプログラム言語で実施されることを特徴とする方法。

【請求項18】請求項10記載の方法であって、前記オブジェクトが、コレクション、索引、パッケージおよびテーブルのいずれかを含むことを特徴とする方法。

【請求項19】データベースのオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するためのデータベースおよび装置を含むコンピュータシステムであって、（a）所与のユーザがア

3

クセス特権を有するオブジェクトの判定を要求するための第１の手段と、（ｂ）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定するための第２の手段と、（ｃ）そのユーザが間接アクセス特権を有するオブジェクトを、（１）そのユーザが属する全部のアクセスグループを自動的に判定するための第４の手段と、（２）第４の手段により判定された前記アクセスグループがアクセス特権を有するオブジェクトを自動的に判定する第５の手段とによって、自動的に判定するための第３の手段との組合せを含むことを特徴とするコンピュータシステム。

【請求項２０】請求項１９記載のシステムであって、前記第３の手段がさらに、公衆がアクセス特権を有するオブジェクトを自動的に判定するための手段を含むことを特徴とするシステム。

【請求項２１】請求項１９記載のシステムであって、さらに、前記ユーザがアクセス特権を有するオブジェクトを表示させるための手段を含むことを特徴とするシステム。

【請求項２２】請求項１９記載のシステムであって、前記第１の手段が、（１）アクセス特権を記述するためにコマンドを発行するための手段と、（２）記述されるオブジェクトの型を述べるための手段と、（３）記述されるオブジェクトの名称を述べるための手段と、（４）アクセス特権情報を受け取る制御ブロックの名称を述べるための手段を含むことを特徴とするシステム。

【請求項２３】請求項１９記載のシステムであって、さらに、（ｆ）前記ユーザがアクセス特権を有する各オブジェクトのアクセス特権が他のユーザに拡張できるかどうかを判定するための手段と、（ｇ）前記ユーザがアクセス特権を有する各オブジェクトのアクセス特権が他のユーザに拡張できるかどうかを表示させるための手段とを含むことを特徴とするシステム。

【請求項２４】請求項１９記載のシステムであって、前記第１、第２および第３の手段が、多数のデータベース製品によって使用するための非手続きコンピュータ言語を実行することを特徴とするシステム。

【請求項２５】請求項１９記載のシステムであって、前記システムが、特定のデータベース製品によって使用するためのアプリケーションプログラミングインタフェースを形成することを特徴とするシステム。

【請求項２６】請求項１９記載のシステムであって、前記オブジェクトが、コレクション、索引、パッケージおよびテーブルを含むことを特徴とするシステム。

【請求項２７】請求項１９記載のシステムであって、前記オブジェクト型が、コレクション、索引、パッケージおよびテーブルの１以上を含むことを特徴とするシステム。

【請求項２８】データベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているア

4

クセス特権を判定するためのコンピュータシステムであって、（ａ）そのユーザがその所与のオブジェクトに対してアクセス特権を有するかの判定を要求するための第１の手段と、（ｂ）そのユーザがそのオブジェクトに対して直接アクセス特権を有するかを自動的に判定するための第２の手段と、（ｃ）そのユーザがそのオブジェクトに対して間接アクセス特権を有するかを、（１）そのユーザが属する全部のアクセスグループを自動的に判定するための第４の手段と、（２）前記第４の手段によって判定されたアクセスグループの１以上がそのオブジェクトに対してアクセス特権を有するかを自動的に判定するための第５の手段とによって、自動的に判定するための第３の手段との組合せを含むことを特徴とするシステム。

【請求項２９】請求項２８記載のシステムであって、前記第３の手段がさらに、公衆がそのオブジェクトに対してアクセス特権を有するかを自動的に判定するための手段を含むことを特徴とするシステム。

【請求項３０】請求項２８記載のシステムであって、さらに、それを通じてユーザがそのオブジェクトに対してアクセス特権を有する各アクセスグループまたは複数のアクセスグループを表示させるための手段を含むことを特徴とするシステム。

【請求項３１】請求項２８記載のシステムであって、前記第１の手段が、（１）アクセス特権を記述するためにコマンドを発行するための手段と、（２）その所与のオブジェクトの型を述べるための手段と、（３）そのオブジェクトの名称を述べるための手段と、（４）アクセス特権情報を受け取る制御ブロックの名称を述べるための手段とを含むことを特徴とするシステム。

【請求項３２】請求項２８記載のシステムであって、さらに、（ｄ）ユーザがそのオブジェクトに対して有するアクセス特権の型を判定するための手段と、（ｅ）前記アクセスの型を表示させるための手段とを含むことを特徴とするシステム。

【請求項３３】請求項２８記載のシステムであって、さらに、（ｆ）そのオブジェクトのアクセス特権が他のユーザに拡張できるかどうかを判定するための手段と、（ｇ）そのオブジェクトのアクセス特権が他のユーザに拡張できるかどうかを表示させるための手段とを含むことを特徴とするシステム。

【請求項３４】請求項２８記載のシステムであって、前記第１、第２および第３の手段が、多数のデータベース製品によって使用するための非手続きコンピュータ言語を実行することを特徴とするシステム。

【請求項３５】請求項２８記載のシステムであって、前記システムが、特定のデータベース製品によって使用するためのアプリケーションプログラミングインタフェースを形成することを特徴とするシステム。

【請求項３６】請求項２８記載のシステムであって、所

5

与のオブジェクトが、コレクション、索引、パッケージおよびテーブルのいずれかを含むことを特徴とするシステム。

【請求項３７】データベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための製品であって、（ａ）その所与のユーザがアクセス特権を有するオブジェクトの判定を要求するための第１のプログラムコード手段と、（ｂ）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定するための第２のプログラムコード手段と、（ｃ）そのユーザが間接アクセス特権を有するオブジェクトを、（１）そのユーザが属する全部のアクセスグループを自動的に判定するための第４のプログラムコード手段と、（２）前記第４のプログラムコード手段により判定された前記アクセスグループがアクセス特権を有するオブジェクトを自動的に判定するための第５のプログラムコード手段とによって、自動的に判定するための第３のプログラムコード手段との組合せを含むことを特徴とする製品。

【請求項３８】請求項３７記載の製品であって、前記第３のプログラムコード手段がさらに、公衆がアクセス特権を有するオブジェクトを自動的に判定するためのプログラムコード手段を含むことを特徴とする製品。

【請求項３９】請求項３７記載の製品であって、さらに、前記ユーザがアクセス特権を有するオブジェクトを表示させるためのプログラムコード手段を含むことを特徴とする製品。

【請求項４０】請求項３７記載の製品であって、前記第１のプログラムコード手段が、（１）アクセス特権を記述するためにコマンドを発行するためのプログラムコード手段と、（２）その所与のオブジェクトの型を述べるためのプログラムコード手段と、（３）そのオブジェクトの名称を述べるためのプログラムコード手段と、（４）アクセス特権情報を受け取る制御ブロックの名称を述べるためのプログラムコード手段とを含むことを特徴とする製品。

【請求項４１】請求項３７記載の製品であって、さらに、（ｆ）前記ユーザがアクセス特権を有する各オブジェクトのアクセス特権が他のユーザに拡張できるかどうかを判定するためのプログラムコード手段と、（ｇ）前記ユーザがアクセス特権を有する各オブジェクトのアクセス特権が他のユーザに拡張できるかどうかを表示させるためのプログラムコード手段とを含むことを特徴とする製品。

【請求項４２】請求項３７記載の製品であって、前記第１、第２および第３のプログラムコード手段が、多数のデータベース製品によって使用するための非手続きコンピュータ言語を形成することを特徴とする製品。

【請求項４３】請求項３７記載の製品であって、前記製品が、特定のデータベース製品によって使用するための

6

アプリケーションプログラミングインタフェースを形成することを特徴とする製品。

【請求項４４】請求項３７記載の製品であって、前記オブジェクトが、コレクション、索引、パッケージおよびテーブルを含むことを特徴とする製品。

【請求項４５】請求項３７記載の製品であって、前記オブジェクト型が、コレクション、索引、パッケージおよびテーブルの１以上を含むことを特徴とする製品。

【請求項４６】データベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための製品であって、（ａ）そのユーザがその所与のオブジェクトに対してアクセス特権を有するかの判定を要求するための第１のプログラムコード手段と、（ｂ）そのユーザがそのオブジェクトに対して直接アクセス特権を有するかを自動的に判定するための第２のプログラムコード手段と、（ｃ）そのユーザがそのオブジェクトに対して間接アクセス特権を有するかを、（１）そのユーザが属する全部のアクセスグループを自動的に判定するための第４のプログラムコード手段と、（２）前記第４のプログラムコード手段により判定されたアクセスグループの１以上がそのオブジェクトに対してアクセス特権を有するかを自動的に判定するための第５のプログラムコード手段とによって、自動的に判定するための第３のプログラムコード手段との組合せを含むことを特徴とする製品。

【請求項４７】請求項４６記載の製品であって、前記第３のプログラムコード手段がさらに、公衆がそのオブジェクトに対してアクセス特権を有するかを自動的に判定するための手段を含むことを特徴とする製品。

【請求項４８】請求項４６記載の製品であって、さらに、それを通じてユーザがそのオブジェクトに対してアクセス特権を有する各アクセスグループまたは複数のアクセスグループを表示させるためのプログラムコード手段を含むことを特徴とする製品。

【請求項４９】請求項４６記載の製品であって、前記第１のプログラムコード手段が、（１）アクセス特権を記述するためにコマンドを発行するためのプログラムコード手段と、（２）その所与のオブジェクトの型を述べるためのプログラムコード手段と、（３）そのオブジェクトの名称を述べるためのプログラムコード手段と、（４）アクセス特権情報を受け取る制御ブロックの名称を述べるためのプログラムコード手段とを含むことを特徴とする製品。

【請求項５０】請求項４６記載の製品であって、さらに、（ｄ）ユーザがそのオブジェクトに対して有するアクセス特権の型を判定するためのプログラムコード手段と、（ｅ）前記アクセスの型を表示させるためのプログラムコード手段とを含むことを特徴とする製品。

【請求項５１】請求項４６記載の製品であって、さらに、（ｆ）そのオブジェクトのアクセス特権が他のユー

7

ザに拡張できるかどうかを判定するためのプログラムコード手段と、（g）そのオブジェクトのアクセス特権が他のユーザに拡張できるかどうかを表示させるためのプログラムコード手段とを含むことを特徴とする製品。

【請求項５２】請求項４６記載の製品であって、前記第１、第２および第３のプログラムコード手段が、多数のデータベース製品によって使用するための非手続きコンピュータ言語を実行することを特徴とする製品。

【請求項５３】請求項４６記載の製品であって、前記製品が、特定のデータベース製品によって使用するためのアプリケーションプログラミングインタフェースを形成することを特徴とする製品。

【請求項５４】請求項４６記載の製品であって、所与のオブジェクトが、コレクション、索引、パッケージおよびテーブルのいずれかを含むことを特徴とする製品。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、データベースのオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための方法に関する。より詳しくは、本発明は、そのような特権を自動的に判定し、かつ、（１）ユーザがアクセス特権を有するオブジェクトの名称、（２）ユーザがアクセス特権を有する各オブジェクトへのアクセスの型の識別、（３）ユーザがそれを通じてアクセス特権を有する関係するアクセスグループの識別、および、（４）そのような特権が他のユーザに拡張できるかどうかに関する識別を表示するための、製品に依存しない方法に関する。

【０００２】

【従来の技術およびその課題】現在、データベースユーザにとって、自己がアクセス特権を有するそのオブジェクトを判定することは極めて困難である。所与のユーザは、例えばデータベースオブジェクトを作成することによりデータベースオブジェクトに「直接アクセス」を、または、当該オブジェクトにアクセスできるグループまたはクラスの構成員となることによりデータベースオブジェクトに対する「間接アクセス」を有することができる。この分類の特殊な例として、データベースユーザが、一般にアクセス可能であるようなデータベースオブジェクトにいつでもアクセスできる場合がある。

【０００３】本明細書で使用する場合、「アクセス特権」は、データベースオブジェクトに対するいずれかの型のアクセスを意味するものとする。こうしたアクセスは、例示であって限定するものではないが、オブジェクトを見る、テーブルの数を変更するなどによりオブジェクトを修正する、オブジェクトの構造を変更するなどによりオブジェクトを変更する、オブジェクトの全部または一部を削除する、といった能力を含むとしてよい。アクセス特権の正式な型は、各種データベース管理システムで標準化されており、当業者には公知である。

8

【０００４】用語「直接アクセス」は、ユーザがグループまたはクラスに関係せずに有する型のアクセス特権を含むものとする。こうした特権は、通常、アクセスされるオブジェクトの所有者または特別に特権を付与された管理者により、ユーザに対して直接許可される。

【０００５】用語「間接アクセス」は、直接ではないすべての型のアクセスを含む。パブリックアクセスは、規定されたグループまたはクラスの構成員によるアクセスであるような「間接アクセス」である。例えば、企業の人事課は、その企業の部外者がアクセスできない一定のデータベースオブジェクト（秘密の人事ファイルなど）へのアクセスが許可されていよう。人事課に転入し、後に転出するような企業雇用者は、その在職中このグループの構成員であり、従ってその人事ファイルに一時的にアクセスできる。

【０００６】従って、グループは、一定のデータベースオブジェクトに対する規定のアクセス特権を備えた「疑似エンティティ」である。これらのグループは、あたかも実際のユーザであるかのようにデータベースで扱われる。

【０００７】所与のデータベースユーザは、１組織内の複数のグループの構成員としてよい。例えば、人事取締役は、その企業内の上位の経営陣グループの構成員と同様、人事グループの構成員としてよい。従って、データベースユーザが、データベース内のアクセスのために自己が属するすべてのグループに気づかない、または、はっきり知らないことは稀ではない。そのグルーピング自体はデータベースの外部で通常に格納されるので、ユーザは、すべての想定されるグループに関する情報および各グループのアクセス特権にアクセスしなくてもよい。

【０００８】従って、ユーザが自己がアクセス特権を有するデータベースオブジェクトの全部を判定することは極めて困難である。所与のユーザは、恐らく、自己が作成し所有するデータベースオブジェクトは知っているであろうが、それらのオブジェクトが膨大になったり、相当以前に作成された場合、たぶん知らないかもしれない。ユーザはまた、自己が１以上のグループの構成員であることは知っているであろうが、自己が属するグループのすべては知らないであろうし、そうしたすべてのグループのアクセス特権を述べることはできないであろう。

【０００９】従って、現在、ユーザは、自己がアクセス特権を有するオブジェクトのすべてを、それらのオブジェクトの特権の型とともに判定し、表示させることは、それが不可能でない場合、困難であることを認めるであろう。

【００１０】実際には、自己のアクセス特権を判定するためにユーザによって要求される情報のすべては、システムのいずれかにおいて入手可能である。しかし、この情報を得るには、ユーザは、データベースそれ自体に対

してだけでなく、システムカタログに対しても多数の照会を行わなければならない。セキュリティグループ構成員の効力などの必要な情報の一部は、セキュリティコードがなければ通常は入手できない。

【００１１】本明細書では、定義を要する多数の付加的な用語が使用される。これらの定義を以下に説明する。

【００１２】データベース「オブジェクト」は、特定の方法で構成されたデータベース内のデータの集合である。例えば、このデータの集合は、「テーブル」または「ビュー」とすることができる。

【００１３】「テーブル」は、行および列で構成されたデータの集合である。

【００１４】「ビュー」は、ユーザがアクセスできるオブジェクトの論理的部分集合である。例えば、テーブルのビューは、そのテーブルの１以外の全部の行を含むことができる。

【００１５】「コレクション」は、データベース内のオブジェクトの集合である。これらのオブジェクトは、例えば、共通の主題に関係することができる。

【００１６】「パッケージ」は、データベースを背景にして走行できる予備処理されたコマンドの集合である。

【００１７】「索引」は、オブジェクト内の基礎をなすオブジェクトである。テーブルの索引はそのテーブルの一部を形成する。

【００１８】「スナップショット」は、時間的に特定の時点のテーブルまたはビューの複写である。例えば、スナップショットは、日に一度だけテーブルから行うことができるが、現在テーブルは連続的に変化している。

【００１９】「ｒｄｂ」は、「関係型データベース」の頭文字語である。

【００２０】「別名」は、データベースのオブジェクトの略称である。例えば、テーブルの公式名を「２７３４．５」とすることができるが、これはユーザが覚えるのは困難である。従って、ユーザは「ｍｙｔａｂ」といった別名をそのテーブルに付けることができる。

【００２１】現在、ＯＳ／２照会マネージャ（ＱＭ）は、アクセス特権判定がＡＳＰ－１の時間枠でテーブルおよびビューについて利用可能であることを要求する。これを行うために、ＱＭは、テーブルのメニューをデータベースユーザに提示し、ユーザはそこから選択できる。ＩＢＭの共通ユーザアクセス（ＣＵＡ）仕様は、これらのメニューがユーザがアクセス可能なテーブルだけを表示することを要する。このガイドラインは、業界および国際規格から導き出されたものであり、最近の人間工学研究に対する回答である。現在、ＱＭは、ＯＳ／２で作用する特殊関数呼出しからこの情報を取得する。

【００２２】

【課題を解決するための手段】本発明の第１の目的は、データベースのオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための方法を提供することである。

【００２３】本発明の第２の目的は、「製品に依存しない」、すなわち、いずれのデータベース管理プログラム製品にも移植できるような、上述の形式の方法を提供することである。

【００２４】本発明の第３の目的は、ユーザがアクセス特権を持たないそうしたテーブルの識別に対するユーザによるアクセスを防止する前述の形式の方法を提供することである。

【００２５】本発明の第４の目的は、多数のデータベースプログラム製品とともに用いるための非手続き言語で実施される前述の形式の方法を提供することである。

【００２６】上述の目的および、後述の説明によって明らかになるであろう他の目的は、本発明に従って、以下の段階を含む方法によって達成される。

【００２７】（ａ）所与のユーザがアクセス特権を有するオブジェクトの判定を要求する。

【００２８】（ｂ）ユーザが直接アクセス特権を有するオブジェクトを自動的に判定する。

【００２９】（ｃ）ユーザが間接アクセス特権を有するオブジェクトを、以下の段階によって自動的に判定する。

【００３０】（１）ユーザが属する全部のアクセスグループを自動的に判定する。

【００３１】（２）段階（１）で判定されたアクセスグループがアクセス特権を有するオブジェクトを自動的に判定する。

【００３２】データベースの特定の単一オブジェクトに関してアクセス特権を判定するために、類似の方法が利用できる。この場合、その方法は以下の段階を含む。

【００３３】（ａ）ユーザがその所与のオブジェクトに対するアクセス特権を有するかどうかの判定を要求する。

【００３４】（ｂ）そのユーザがそのオブジェクトに対する直接アクセスを有するかどうかを自動的に判定する。

【００３５】（ｃ）そのユーザがそのオブジェクトに対する間接アクセスを有するかどうかを、以下の段階によって自動的に判定する。

【００３６】（１）ユーザが属する全部のアクセスグループを自動的に判定する。

【００３７】（２）段階（１）で判定されたアクセスグループの１以上がそのオブジェクトに対するアクセス特権を有するかどうかを自動的に判定する。

【００３８】こうして得られたアクセス特権情報は、（例えばモニタまたは印刷のいずれかによって）ユーザに表示するか、または、他のいずれかの方法によって直接使用することができる。例えば、アクセス特権を表示するのではなく、これらの特権を認証機構として使用し、ユーザに、自己が指定したオブジェクトへの直接ア

クセスを付与することが可能である。あるいはまた、その情報を、そのユーザの特権の直接表示を必要としない統計その他の目的のために使用することができる。

【００３９】従来、同種のアクセス特権情報を取得するには、ユーザは、自己が属するグループを判定してから、それらのグループがどのオブジェクトにアクセスできるかを判定する必要があった。この第２の段階は、アクセスの型とともに、そのデータベースの各オブジェクトに対してアクセスできるすべての人間およびグループのリストを含むカタログで照会する必要があった。そうしたカタログは、各グループの人間のリストは含まないので、グループ管理ユーティリティ（データベース外部の）に対する照会によってこの事実を個別に判定しなければならなかった。

【００４０】本発明は、このプロセスを自動化し、ユーザがカタログを見ることによりデータベースの全オブジェクトのリストを見させなくすることを保証する。

【００４１】本発明の一つの特長に従えば、この方法はまた、公衆がアクセス特権を有するオブジェクトを自動的に判定し、それによりユーザが直接および間接アクセスを行えるオブジェクトのリスト中にそうしたオブジェクトを含めることができる。

【００４２】本発明の他の特長に従えば、ユーザのアクセス特権の判定を要求する段階は、以下の段階を含むことができる。

【００４３】（１）アクセス特権を記述するためにコマンドを発行する
（２）記述されるオブジェクトの型を述べる
（３）記述されるオブジェクトの名称を述べる
（４）アクセス特権情報を受け取る制御ブロックの名称を述べる
あるオブジェクトに対するアクセス特権があるアクセスグループによって許可されると、その各アクセスグループは好ましくはそのオブジェクトとともに表示される。

【００４４】本発明の他の特長に従えば、ユーザがアクセス特権を有する各オブジェクトへのアクセスの型は、各オブジェクトとともに表示される。アクセスのそうした型は、例えば、「選択」、「挿入」、「更新」、「削除」、「ドロップ」、「変更」、「索引」および「参照」アクセスを含むことができる。これらのアクセスの型は、当技術分野で十分に定義され認識されている。

【００４５】本発明のさらに好ましい特長に従えば、ユーザがアクセス特権を有する各オブジェクトについて、そのアクセス特権が他のユーザに拡張できるかどうかを判定する段階が含まれる。この情報は、ユーザの選択により、表示または他の方法でユーザによって使用することができる。

【００４６】本発明の他の特長に従えば、この方法は、構造化照会言語（ＳＱＬ）などの非手続き言語で実施される。あるいはまた、この方法は、アプリケーションプログラミングインタフェース（ＡＰＩ）で実施してもよい。ＳＱＬの使用は、この方法をいずれのデータベース管理製品に移植させることが可能になる。

【００４７】上述の方法および特長は、コンピュータシステムで走行するように設計された適切なプログラムコードによって実施される。このようなプログラムコードおよびコンピュータシステムは、本発明の範囲に含まれるものとする。

【００４８】本発明の好ましい実施例を添付図面によって以下に説明する。

【００４９】
【実施例】本発明の好ましい実施例を図１～５によって説明する。

【００５０】図１は、本発明の概略的なコンピュータハードウエア環境を示す。本発明は、単一のパーソナルコンピュータ、情報を交換するために一体に接続された２以上のパーソナルコンピュータ、または、図１に示すように、ＩＢＭ　３７０システムなどのホストコンピュータおよび相互に一体に接続された２以上のパーソナルコンピュータで実施することができる。図１は、大型ディスク記憶ファイル１２とともに動作するホストコンピュータ１０を例示する。ホストコンピュータ１０には、それぞれ、データおよび制御情報を搬送する多数の回線１８および２０によって第１のパーソナルコンピュータ１４および第２のパーソナルコンピュータ１６が接続されている。これらの２のパーソナルコンピュータもデータおよび制御情報回線２２によって相互に接続されている。

【００５１】本発明のデータベース環境は、図２に例示した形態をとることができる。この場合、ＰＳ／２（登録商標）パーソナルコンピュータは、関係型テーブル構造およびデータの交換を可能にする統合交換フォーマット（ＩＸＦ）データ交換ソフトウエアのＯＳ／２拡張版（登録商標）データベースマネージャ適応機能とともに動作する。文字データは、ＩＢＭのＡＳＣＩＩコードページ４３７などの特定のコードページ環境で１以上のデータベースに格納される。数値および日付／時間データは、基本オペレーティングシステムおよび／またはハードウエアが支援するフォーマットで内部的に格納される。

【００５２】詳しくは、このデータベースマネージャは、全部のデータがテーブルのコレクションとしてビューされる関係型データベースモデルを支援するデータベース管理システム（ハードウエアおよびソフトウエア）である。データベースマネージャは、「データベースサービス」と称する関係型コマンドプロセッサ、データを見つけるための汎用照会システム、他のコンピュータシステムとのデータ交換のためのシステム、ならびに、個々の関係型データベースのバックアップ、復元および保守のためのシステムを付与する。

13

【００５３】データベースサービスは、データベースマネージャの関係型コマンドプロセッサである。これは、記憶アクセス用システム、構造化照会言語（ＳＱＬ）命令文処理、データベース管理、ロック管理、並行性制御、ライトアヘッドロギング、回復サービス、行レベルロッキング細分性、また、アプリケーション、システムおよび記録媒体の障害事象におけるデータ回復、ならびに、機密保護制御を含む多数の機能にサービスする。データベースマネージャおよびデータベースサービスの両者ともＰＳ／２コンピュータ用の公知のアプリケーションであり、詳述する必要はない。

【００５４】図３は、個別のオブジェクト２３および２４および、オブジェクトのグループまたはコレクション２５、２６および２７を含む通常のデータベースを示す。例えば、オブジェクト２３は索引２８が付けられているが、オブジェクト２４は索引を持っていない。コレクション２５～２７はそれぞれ、多数のオブジェクト２９、３０および３１を含む。

【００５５】所与のオブジェクトに対するアクセスの各種の型は、図４に例示するユーザの全集合によって得られる。データベースオブジェクトに対するアクセスは、ユーザ３２、３３および３４によって図示されたように直接アクセス、または、グループ３６および３８ならびにそれぞれの構成員ユーザ４０および４２によって図示されたように間接アクセスとすることができる。あるいはまた、オブジェクトに対するパブリックアクセスをパブリックアクセス「グループ」４６を通じて全ユーザ４４に付与することができる。

【００５６】図５は、プログラミング命令「ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ」をコンピュータ内で実行できる方法を示す流れ図である。このアルゴリズムでは、初期化時に、データベースが以下の情報にアクセスすることを前提とする。

【００５７】（１）現アプリケーションを走行しているユーザのログイン識別

（２）ユーザが属するグループＧ１，Ｇ２，．．．，Ｇｊ，．．．，ＧＮ（０＜＝Ｎ）

データベースプロセッサは、＜オブジェクトセット＞に関する命令「ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ」を受け取ると、＜オブジェクトセット＞をオブジェクトＢ１，Ｂ２，．．．，Ｂｉ，．．．，ＢＭ（０＜Ｍ）のリストにパーズする（ブロック５１）。その後、プログラムは、ヘッダを初期化し（ブロック５２）、各オブジェクトＢｉをうまく見つけるためにループに入る（ブロック５３）。ループでは、特権マスクが初期化され（ブロック５４）、現在オブジェクトＢｉに対してユーザによって保持されている特権に対応するフラグが設定される（ブロック５５）。

14

【００５８】プログラムは次に、ユーザが属するグループＧｊのそれぞれを検討するためにループに入る（ブロック５６）。各グループについて、現在オブジェクトＢｉに対して特定のグループによって保持されている特権に対応するフラグが設定される（ブロック５７）。すべてのグループが検討されると（ブロック５９）、現在オブジェクトＢｉに対して公衆によって保持されている特権に対応するフラグが設定される（ブロック６０）。すべてのオブジェクトが検討されると（ブロック６０）、設定されたフラグによって定義された情報がアプリケーションプログラムに送られる（ブロック６１）。このデータは、希望に応じて、アプリケーションプログラムによって表示させたり、または分析させたりすることができる。ＳＱＬでの実施本発明の構造化照会言語（ＳＱＬ）での特定の実施例を以下に説明する。ＳＱＬは、多くのデータベース製品により使用できる公知の非手続き言語である。

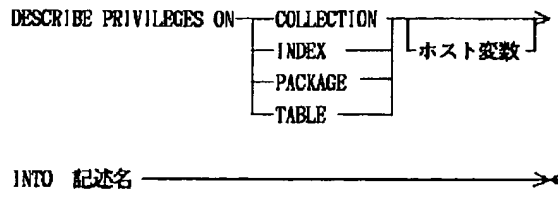
【００５９】ＳＱＬでのＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ命令文は、現在のデータベースの例（すなわち、ＣＵＲＲＥＮＴ　ＳＥＲＶＥＲ特殊レジスタにリスト化されているデータベースの例）で、その命令文の実行者によって現在保持されている特権に関する情報を入手する。

【００６０】以下使用される用語「一次許可識別」は、特殊レジスタ「ＵＳＥＲ」の値を意味するものとする。「二次許可識別」は、データ操作言語が実行される時に特権を判定する際に一次許可識別に加えて使用される許可識別である。「活性許可識別」は、命令文を実行するユーザの許可識別である。これは、ＳＱＬＩＤ特殊レジスタ（それを支援する製品の場合）の値またはＵＳＥＲの値のいずれかである。「命令文の許可識別」は、上述のいずれにも当てはまらず、ＤＥＳＣＲＩＢＥＰＲＩＶＩＬＥＧＥＳ命令文がそれに拘束されていた許可識別をいう。最後に、「コレクション識別」は、３部分から成るオブジェクト名の中央部分として使用される識別子である。

【００６１】ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ命令文は、アプリケーションプログラムで埋め込まれるだけである。これは動的に作成できない実行文である。命令文の許可識別によって保持された特権は、管理権限を含まなければならない。

【００６２】ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ命令文は、以下の形態をとる。

【表１】



この命令文における「ON」は、記述されるオブジェクトの型を識別する。オプションには、好ましくは、以下を含む。

【００６３】（１）ＣＯＬＬＥＣＴＩＯＮ：コレクションに関する特権が記述される。

【００６４】（２）ＩＮＤＥＸ：索引に関する特権が記述される。

【００６５】（３）ＰＡＣＫＡＧＥ：パッケージに関する特権が記述される。

【００６６】（４）ＴＡＢＬＥ：テーブル、ビューおよびスナップショットに関する特権が記述される。

【００６７】ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ＊命令文において、「ホスト変数」は、特権が記述されるオブジェクトを識別する。ホスト変数の値は、以下の表１に示す形式を有し、ホスト変数内で左寄せされており、区切り識別子内での空白を除き、空白をまったく含まない文字列である。名称の長さが変数の長さより小さい場合、名称の最終文字の後に空白が続く。デフォールト値は「＊」である。表の用語「ｒｄｂ」は、「関係型データベース」を意味する。

【００６８】ホスト変数は、文字列変数を宣言するための規則のもとでの呼出しプログラムで記述される。インジケータ変数は指定する必要がない。

【表２】

表１　オブジェクト指定の有効形式

形　式	意　味
ＯＮ文節がＣＯＬＬＥＣＴＩＯＮを指定しない場合	
rdb 名、コレクション識別、オブジェクト名 コレクション識別、オブジェクト名 オブジェクト名	単一オブジェクト（テーブルもしくはビュー、索引、パッケージまたはスナップショット）、または、オブジェクトの別名
rdb 名、コレクション識別★ コレクション識別★ ★	その中央識別子が特定のコレクション識別である所与の型の全オブジェクト
rdb 名★★ ★★	データベース例の所与の型の全オブジェクト
ＯＮ文節がＣＯＬＬＥＣＴＩＯＮを指定する場合	
rdb 名、コレクション識別 コレクション識別	単一コレクション
rdb 名★ ★	データベース例の全コレクション

各形式において、ｒｄｂ名が指定された場合、それは現在のデータベース例の名称（すなわち、ＣＵＲＲＥＮＴ　ＳＥＲＶＥＲの値）である。ｒｄｂ名が指定されない場合、それは現在のデータベース例の名称としてみなされる。

【００６９】コレクション識別が指定されず、オブジェクトの型がＣＯＬＬＥＣＴＩＯＮではない場合、コレクション識別は、ＣＵＲＲＥＮＴ　ＣＯＬＬＥＣＴＩＯＮの実行時間値（支援されている場合）、または、他の場合にはＵＳＥＲの実行時間値としてみなされる。

【００７０】「ＩＮＴＯ」は、ＳＱＬ特権領域（ＳＱＬＰＡ）を名づける。ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ命令文が実行される場合、後述の表２～４に従ってＳＱＬＰＡのフィールドに値が割り当てられる。

【００７１】テーブルのフィールドを識別するために使用される名称は、これらのフィールドを指示するために

17

プログラムで使用される名称である必要はない。しかし、それらは、プログラム言語「C」ではそれらの名称が小文字となる点を除き、INCLUDE SQLPA

18

によって作成される構造で使用されている名称であろう。

【表3】

表2 SQLPAの説明

これらのフィールドの値は、SQLPANフィールドを除き、システムによって割り当てられ、DESCRIBE PRIVILEGES命令文を発行する以前に呼出しアプリケーションによって付与されなければならない。

フィールド	データ型	用法
SQLPAID	CHAR(8)	アイキャッチャおよび記述子の生成:'SQLPAID'
SQLPABC	整数	SQLPA のバイト単位の長さ。これは32+64*SQLPA となる。
SQLPAN	整数	呼出しアプリケーションによりSQLPA で空間が予約されているオブジェクト記述の総数。これは命令文実行前に記入されなければならないSQLPA のうちの唯一のフィールドである。
SQLPAD	整数	返されるはずのオブジェクトの実数。
SQLPRES	CHAR(12)	将来用に予約。
SQLPAR	構造	ON文節およびホスト変数の指定を一致させるオブジェクトの反復リスト。記述については表3を参照。

【表4】

表3 SQLPAR記述

フィールド	データ型	用法
SQLPCOL	CHAR(18)	ON文節がCOLLECTIONを指定しない場合、記述されるオブジェクトのコレクション識別であり、右側に空白が埋められる。ON文節がCOLLECTIONを指定する場合、このフィールドは空白である。
SQLPOBJ	CHAR(18)	記述されるオブジェクトの名称であり、右側に空白が埋められる。オブジェクトを指定するため別名が使用される場合、別名がオブジェクトを名づけられるためにここで使用され、SQLPALS は「Y」に設定される。
SQLPALS	CHAR(1)	SQLADBJ で指定された名称が別名である場合「Y」、そうでなければ「N」。
SQLPOTP	CHAR(1)	オブジェクト型 C コレクション識別 I 索引 P パッケージ S スナップショット T テーブル V ビュー
SQLPOWN	CHAR(1)	ユーザがそのオブジェクトを所有しているか、または、CONTROL 特権を有する場合は「Y」、そうでなければ「N」。
SQLPPRVS	CHAR(25)	記述されるオブジェクトのDESCRIBE PRIVILEGES コマンドの実行者によって保持された特権を記述する文字列。有効値は以下を含む。 「Y」ユーザは特権を有しているが、GRANT OPTIONは伴わない。 「G」ユーザはGRANT OPTIONを伴う特権を有している 「N」ユーザは特権を持たない。 空白 特権は適用されない、または、将来用に予約されている。 表4は隠オブジェクトについて記述される特権を示す。

【表5】

19 20

表4 各オブジェクト型のSQLPRVS 定義
バイト10－25は将来用に予約されている。
SQLPOTP=T の場合、全バイトは予約される。
特権がテーブルまたはビューの1以上のカラムに存在する場合は、
REFERENCE およびUPDATEは記録される。

バイト	コレクション	パッケージ	スナップショット	テーブル	ビュー
1	USE	DESCRIBE	SELECT	SELECT	SELECT
2	CREATE	PREPARE	Reserved	INSERT	INSERT
3	Reserved	EXECUTE	Reserved	UPDATE	UPDATE
4	DROP OBJECT	DROP STATEMENT	Reserved	DELETE	DELETE
5	DROP	DROP	DROP	DROP	DROP
6	Reserved	BIND	ALTER	ALTER	Reserved
7	Reserved	REBIND	INDEX	INDEX	Reserved
8	Reserved	COPY	Reserved	REFERENCE	Reserved
9	Reserved	Reserved	REFRESH	Reserved	Reserved

特権の判定は、活性許可識別に直接付与されたＧＲＡＮＴＳにだけ依存するものではない。一次および二次許可識別のＧＲＡＮＴＳ、ＧＲＡＮＴＳ　ＰＵＢＬＩＣ、活性許可識別によって保持されている管理権限が考慮される。その決定は機能による。すなわち、ユーザ実行の場合、ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ命令文はその特権によって限定された機能を現在的に実行できる。すべての関連する特殊レジスタの値が与えられていれば、ユーザは特権を持っているとみなされる。例えば、活性許可識別がオブジェクトの所有者である場合、全フラグは通常、「Ｇ」に設定される。

【００７２】ＧＲＡＮＴオプションを持たないＯＳ／２においても、ユーザがオブジェクトの所有者である場合、機能上、ユーザはそのオブジェクトに対する許可特権を有する。

【００７３】ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳのさらに別の使用例として、コレクションに対するＣＲＥＡＴＥおよびＤＲＯＰ＿ＯＢＪＥＣＴ特権を検討しよう。

【００７４】（１）ＤＢ２およびＳＱＬ／ＤＳにおいて、これらの特権は両者とも、そのコレクションのコレクション識別が活性許可識別と同一でない限り、または、それらのバイトを「Ｙ」に設定させることになるＤＢ２でのＳＹＳＡＤＭまたはＤＢＡＤＭ権限またはＳＱＬ／ＤＳでのＤＢＡ権限をユーザが有していない限り、「Ｎ」に設定される。

【００７５】（２）ＯＳ／２では、これらの特権は常に「Ｙ」である。

【００７６】（３）ＯＳ／４００では、これらの特権は、そのコレクションに対するユーザの特権に応じて変化する。

【００７７】ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ命令文を実行するユーザがオブジェクトに対していずれの特権も持たない場合、そのオブジェクトはＳＱＬＰＡにリスト化されない。単一オブジェクトだけが指定され、ユーザがこのオブジェクトに対する特権をまったく持たない場合、エラーが返される。

【００７８】ＳＱＬＰＡＮによって示されたＳＱＬＰＡＲブロックの数だけが返される。しかし、ＳＱＬＰＡＤは常に、返されることができたはずのＳＱＬＰＡＲブロックの総数を示すように設定される。

【００７９】ＳＱＬＰＡＮがゼロに設定されている場合、ＳＱＬＰＡＲブロックをまったく持たないＳＱＬＰＡが返される。これは、ＳＱＬＰＡＤが設定されるので、ＳＱＬＰＡに必要な空間量を事前に決定するためにアプリケーションにより使用することができる。しかし、特権の計算が２度行われる必要があるので、これは高価なプロセスとなり、勧められない。アプリケーションプログラマは、代わりに、ＳＱＬＰＡＮについて合理的な値を選択し、必要な場合にのみＤＥＳＣＲＩＢＥＰＲＩＶＩＬＥＧＥＳコマンドを再付託するように努めるべきである。

【００８０】ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ命令文には以下の例外が適用される。

【００８１】（１）ホスト変数の内容が有効形式のいずれかに一致しない場合、ＳＱＬＳＴＡＴＥ　３５５０２（「名称無効文字」）が返される。

【００８２】（２）ｒｄｂ名が局所データベース例の名称に一致しない場合、ＳＱＬＳＴＡＴＥ　５６０２３（「遠隔オブジェクトの無効参照」）が返される。

【００８３】（３）ＳＱＬＰＡＮが負数を指定したかまたは完全にアドレス指定できない場合、ＳＱＬＳＴＡＴＥ　５１００１（「無効呼出しパラメータリスト／制御ブロック」）が返される。

【００８４】（４）単一のオブジェクトが指定され、そのオブジェクトが存在しない場合、または、特定のコレクション識別が指定され、そのコレクションが存在しない場合、ＳＱＬＳＴＡＴＥ　５２００４（「未定義オブ

ジェクト／制約条件名」）が返される。

【００８５】（５）単一のオブジェクトが指定され、ＤＥＳＣＲＩＢＥ　ＰＲＩＶＩＬＥＧＥＳ命令文を実行するユーザがそのオブジェクトに対する特権を持たない場合、ＳＱＬＳＴＡＴＥ　５９００１（「許可識別が指定オブジェクトの指定動作を実行するための特権を持たない」）が返される。

実施例

例えば、遠隔のデータベースに、ＲＡＢＢＩＴの識別子のもとで３のテーブルが存在し、それぞれの名称をＦＬＯＰＳＹ，ＭＯＰＳＹおよびＣＯＴＴＯＮＴＡＬＬとする。また、ＶＥＧＥＴＡＢＬＥ＿ＧＡＲＤＥＮと称する

ビューもある。

【００８６】ユーザＰＥＴＥＲはＦＬＯＰＳＹの所有者であり、ＰＥＴＥＲはＭＯＰＳＹへのＳＥＬＥＣＴアクセスを許可されている。ＰＥＴＥＲはＶＥＧＥＴＡＢＬＥ＿ＧＡＲＤＥＮに直接アクセスすることはできないが、ＶＥＧＥＴＡＢＬＥ＿ＧＡＲＤＥＮにＵＰＤＡＴＥおよびＤＥＬＥＴＥアクセスができるＢＡＤ＿ＢＵＮＮＩＥＳと称するグループに属している。

【００８７】ＰＥＴＥＲは、ＢＡＤ＿ＢＵＮＮＩＥＳ全体の選択言語であるＣ言語で以下のプログラムをコード化した。

```
EXEC SQL INCLUDE SQLPA;
EXEC SQL INCLUDE SQLCA;
EXEC SQL BEGIN DECLARE SECTION;
  char hostvar[9]="RABBIT.* "3
EXEC SQL END DECKARE SECTION;
main()
 {
struct sqlpa* aa; /* INCLUDE は例ではなく、構造だけを定義する* /
char buffer[32+5* 64];/* 5のSQLPARブロックについて十分な空間がある*
/
aa=buffer;
aa-)sqlpan=5; /* SQLPANを５ブロックの余地を示すために設定する* /
EXEC SQL
  DESCRIBE PRIVILEGES ON TABLE:hostvar INTO:* aa;
    .
    .
    .
}
The results were:    sqlpabc              224
sqlpan                 5
sqlpad                 3
sqlpar[0].sqlpcol      "RABBIT"
sqlpar[0].sqlpobj      "FLOPSY"
sqlpar[0].sqlpals      "N"
```

```
sqlpar[0].sqlpotp       "T"
splpar[0].sqlpown       "Y"
sqlpar[0].sqlpprvs[0]   "G" /* 選択* /
sqlpar[0].sqlpprvs[1]   "G" /* 挿入* /
sqlpar[0].sqlpprvs[2]   "G" /* 更新* /
sqlpar[0].sqlpprvs[3]   "G" /* 削除* /
sqlpar[0].sqlpprvs[4]   "Y" /* ドロップ* /
/* OS/400 はドロップについて"G" を返す* /
sqlpar[0].sqlpprvs[5]   "G" /* 変更* /
sqlpar[0].sqlpprvs[6]   "G" /* 検印* /
sqlpar[0].sqlpprvs[7]   "G" /* 参照* /
sqlpar[0].sqlpprvs[8]   " "  /* 予約* /
sqlpar[1].sqlpcol       "RABBIT"
sqlpar[1].sqlpobj       "MOPSY"
sqlpar[1].sqlpals       "N"
sqlpar[1].sqlpotp       "T"
sqlpar[1].sqlpown       "N"
sqlpar[1].sqlpprvs[0]   "Y" /* 選択* /
sqlpar[1].sqlpprvs[1]   "N" /* 挿入* /
sqlpar[1].sqlpprvs[2]   "N" /* 更新* /
sqlpar[1].sqlpprvs[3]   "N" /* 削除* /
sqlpar[1].sqlpprvs[4]   "N" /* ドロップ* /
sqlpar[1].sqlpprvs[5]   "N" /* 変更* /
sqlpar[1].sqlpprvs[6]   "N" /* 索引* /
sqlpar[1].sqlpprvs[7]   "N" /* 参照* /
sqlpar[1].sqlpprvs[8]   " " /* 予約* /
    .
    .
    .
sqlpar[2].sqlpcol       "RABBIT"
sqlpar[2].sqlpobj       "VEGETABLE GARDEN"
sqlpar[2].sqlpals       "N"
sqlpar[2].sqlpotp       "V"
sqlpar[2].sqlpown       "N"
sqlpar[2].sqlpprvs[0]   "N" /* 選択* /
sqlpar[2].sqlpprvs[1]   "N" /* 挿入* /
sqlpar[2].sqlpprvs[2]   "Y" /* 更新* /
sqlpar[2].sqlpprvs[3]   "Y" /* 削除* /
sqlpar[2].sqlpprvs[4]   "N" /* ドロップ* /
sqlpar[2].sqlpprvs[5]   " " /* 変更* /
sqlpar[2].sqlpprvs[6]   " " /* 索引* /
sqlpar[2].sqlpprvs[7]   " " /* 参照* /
sqlpar[2].sqlpprvs[8]   " " /* 予約* /
```

【００８８】本発明は上述したように、データベースのオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための方法であって、（ａ）所与のユーザがアクセス特権を有するオブジェクトの判定を要求する段階と、（ｂ）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定する段階と、（ｃ）そのユーザが間接アクセス特権を有

するオブジェクトを、（１）そのユーザが属する全部のアクセスグループを自動的に判定する段階と、（２）段階（１）で判定された前記アクセスグループがアクセス特権を有するオブジェクトを自動的に判定する段階によって、自動的に判定する段階とを含んでいる。ここで、さらに、前記ユーザがアクセス特権を有するオブジェクトを表示させる段階と、前記アクセスグループがアクセス特権を有するオブジェクトとともにその関係アクセスグループを表示する段階とを含んでいてもよい。本発明は、アクセス特権を判定する方法であって、さらに（ｄ）前記ユーザがアクセス特権を有する各オブジェクトへのアクセスの型を判定する段階と、（ｅ）各自のオブジェクトとともに前記アクセスの型を表示させる段階とを含んでいてもよい。さらに、前記アクセスの型が、選択、挿入、更新、削除、ドロップ、変更、索引および参照のうちの１以上を含んでいてもよい。あるいは本発明の方法は、さらに、（ｆ）前記ユーザがアクセス特権を有する各オブジェクトのアクセス特権が他のユーザに拡張できるかどうかを判定する段階と、（ｇ）前記ユーザがアクセス特権を有する各オブジェクトのアクセス特権が他のユーザに拡張できるかどうかを表示させる段階とを含んでいてもよい。ここで、前記方法が、多数のデータベース製品によって使用するための非手続きコンピュータ言語で実施される場合に、前記非手続き言語が構造化照会言語（ＳＱＬ）であってもよい。本発明のアクセス特権を判定する方法であって、前記要求段階が、（１）アクセス特権を記述するためにコマンドを発行する段階と、（２）記述されるオブジェクトの型を述べる段階と、（３）記述されるオブジェクトの名称を述べる段階と、（４）アクセス特権情報を受け取る制御ブロックの名称を述べる段階とを含み、前記要求段階が、アクセス特権が要求されるオブジェクトの型を指定する段階を含んでいてもよい。また、本発明のデータベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための方法は、（ａ）そのユーザがその所与のオブジェクトに対してアクセス特権を有するかの判定を要求する段階と、（ｂ）そのユーザがそのオブジェクトに対して直接アクセス特権を有するかを自動的に判定する段階と、（ｃ）そのユーザがそのオブジェクトに対して間接アクセス特権を有するかを、（１）そのユーザが属する全部のアクセスグループを自動的に判定する段階と、（２）段階（１）で判定されたアクセスグループの１以上がそのオブジェクトに対してアクセス特権を有するかを自動的に判定する段階によって、自動的に判定する段階とを含んでいてもよい。そして、そのアクセス特権を判定するための方法は、さらに、（ｄ）ユーザがそのオブジェクトに対して有するアクセス特権の型を判定する段階と、（ｅ）前記アクセスの型を表示させる段階とを含み、前記アクセスの型が、選択、挿入、更新、削除、ドロッ

プ、変更、索引および参照のうちの1以上を含む方法であってもよい。前記方法は、多数のデータベース製品によって使用するための非手続きコンピュータ言語で実施される場合、前記非手続き言語が構造化照会言語（SQL）であってもよい。また本発明は、データベースのオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するためのデータベースおよび装置を含むコンピュータシステムであって、（a）所与のユーザがアクセス特権を有するオブジェクトの判定を要求するための第1の手段と、（b）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定するための第2の手段と、（c）そのユーザが間接アクセス特権を有するオブジェクトを、（1）そのユーザが属する全部のアクセスグループを自動的に判定するための第4の手段と、（2）第4の手段により判定された前記アクセスグループがアクセス特権を有するオブジェクトを自動的に判定する第5の手段とによって、自動的に判定するための第3の手段との組合せを含むことを特徴とするコンピュータシステムであってもよい。このシステムは、さらに、前記ユーザがアクセス特権を有するオブジェクトを表示させるための手段と、前記アクセスグループがアクセス特権を有するオブジェクトとともにその関係アクセスグループを表示するための手段を含んでいてもよい。さらに、このシステムは、（d）前記ユーザがアクセス特権を有する各オブジェクトへのアクセスの型を判定するための手段と、（e）各自のオブジェクトとともに前記アクセスの型を表示させるための手段とを含んでいてもよい。また前記アクセスの型が、選択、挿入、更新、削除、ドロップ、変更、索引および参照のうちの1以上を含んだシステムであってもよい。このシステムにおいて、前記第1、第2および第3の手段が、多数のデータベース製品によって使用するための非手続きコンピュータ言語を実行することを特徴とする場合は、前記非手続き言語が構造化照会言語（SQL）であってもよい。ここで、前記第1の手段が、（1）アクセス特権を記述するためにコマンドを発行するための手段と、（2）記述されるオブジェクトの型を述べるための手段と、（3）記述されるオブジェクトの名称を述べるための手段と、（4）アクセス特権情報を受け取る制御ブロックの名称を述べるための手段を含む場合、前記第1の手段が、アクセス特権が要求されるオブジェクトの型を指定するための手段を含むシステムであってもよい。また、本発明はデータベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するためのコンピュータシステムであって、（a）そのユーザがその所与のオブジェクトに対してアクセス特権を有するかの判定を要求するための第1の手段と、（b）そのユーザがそのオブジェクトに対して直接アクセス特権を有するかを自動的に判定するための第2の手段と、（c）そのユーザがそのオブジェクトに対して間接アクセス特権を有するかを、（1）そのユーザが属する全部のアクセスグループを自動的に判定するための第4の手段と、（2）前記第4の手段によって判定されたアクセスグループの1以上がそのオブジェクトに対してアクセス特権を有するかを自動的に判定するための第5の手段とによって、自動的に判定するための第3の手段との組合せを含むことを特徴とするシステムであってもよい。このシステムは、さらに、（d）ユーザがそのオブジェクトに対して有するアクセス特権の型を判定するための手段と、（e）前記アクセスの型を表示させるための手段とを含み、前記アクセスの型が、選択、挿入、更新、削除、ドロップ、変更、索引および参照のうちの1以上を含んでいてもよい。また、このような本発明のシステムは、前記第1、第2および第3の手段が、多数のデータベース製品によって使用するための非手続きコンピュータ言語を実行する場合、前記非手続き言語が構造化照会言語（SQL）であってもよい。また、本発明はデータベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための製品であって、（a）その所与のユーザがアクセス特権を有するオブジェクトの判定を要求するための第1のプログラムコード手段と、（b）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定するための第2のプログラムコード手段と、（c）そのユーザが間接アクセス特権を有するオブジェクトを、（1）そのユーザが属する全部のアクセスグループを自動的に判定するための第4のプログラムコード手段と、（2）前記第4のプログラムコード手段により判定された前記アクセスグループがアクセス特権を有するオブジェクトを自動的に判定するための第5のプログラムコード手段とによって、自動的に判定するための第3のプログラムコード手段との組合せを含むことを特徴とする製品であってもよい。本発明の製品は、さらに、前記ユーザがアクセス特権を有するオブジェクトを表示させるためのプログラムコード手段と、前記アクセスグループがアクセス特権を有するオブジェクトとともにその関係アクセスグループを表示するためのプログラムコード手段とを含んでいてもよい。さらに、本発明の製品は、（d）前記ユーザがアクセス特権を有する各オブジェクトに対するアクセスの型を判定するためのプログラムコード手段と、（e）前記アクセスの型を各自のオブジェクトとともに表示させるためのプログラムコード手段とを含んでいてもよく、さらに、前記アクセスの型が、選択、挿入、更新、削除、ドロップ、変更、索引および参照のうちの1以上を含むものであってもよい。ここで、前記第1、第2および第3のプログラムコード手段が、多数のデータベース製品によって使用するための非手続きコンピュータ言語を形成する場合は、前記非手続き言語が構造化照会言語（SQL）であってもよい。また本発明の製品は、前記第1

27

のプログラムコード手段が、（1）アクセス特権を記述するためにコマンドを発行するためのプログラムコード手段と、（2）その所与のオブジェクトの型を述べるためのプログラムコード手段と、（3）そのオブジェクトの名称を述べるためのプログラムコード手段と、（4）アクセス特権情報を受け取る制御ブロックの名称を述べるためのプログラムコード手段とを含み、前記第1のプログラムコード手段が、アクセス特権が要求されるオブジェクトの型を指定するための手段を含んでいてもよい。また、本発明の製品は、データベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための製品であって、（a）そのユーザがその所与のオブジェクトに対してアクセス特権を有するかの判定を要求するための第1のプログラムコード手段と、（b）そのユーザがそのオブジェクトに対して直接アクセス特権を有するかを自動的に判定するための第2のプログラムコード手段と、（c）そのユーザがそのオブジェクトに対して間接アクセス特権を有するかを、（1）そのユーザが属する全部のアクセスグループを自動的に判定するための第4のプログラムコード手段と、（2）前記第4のプログラムコード手段により判定されたアクセスグループの1異常がそのオブジェクトに対してアクセス特権を有するかを自動的に判定するための第3のプログラムコード手段と、（d）ユーザがそのオブジェクトに対して有するアクセス特権の型を判定するためのプログラムコード手段と、（e）前記アクセスの型を表示させるためのプログラムコード手段とを含み、前記アクセスの型が、選択、挿入、更新、削除、ドロップ、変更、索引および参照のうちの1以上を含んでいてもよい。前記第1、第2および第3のプログラムコード手段が、多数のデータベース製

28

品によって使用するための非手続きコンピュータ言語を実行する場合は、前記非手続き言語が構造化照会言語（ＳＱＬ）であってもよい。

【図面の簡単な説明】

【図1】ホストコンピュータおよび2つのパーソナルコンピュータを含む小型コンピュータシステムを示すブロック図。

【図2】データベースマネージャおよび2つの個別データベースを支援するオペレーティングシステムを用いたパーソナルコンピュータシステムのブロック図。

【図3】データベースに含まれる多数のオブジェクトを例示する説明図。

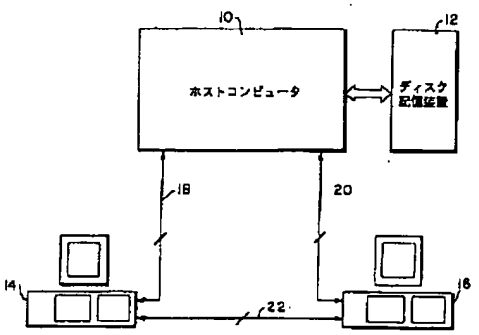
【図4】データベースへのユーザアクセスを例示する説明図。

【図5】本発明に従った方法を実施するためのアルゴリズムの流れ図。

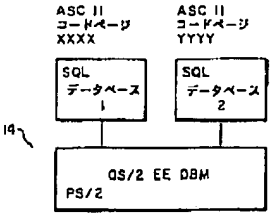
【符号の説明】

10　ホストコンピュータ
12　ディスク記憶装置
14　第1のパーソナルコンピュータ
16　第2のパーソナルコンピュータ
18，20　回線
22　データおよび制御情報回線
23，24，29～31　オブジェクト
25～27　コレクション
28　索引
32～34　ユーザ
36，38，46　グループ
40，42　構成員ユーザ
44　全ユーザ

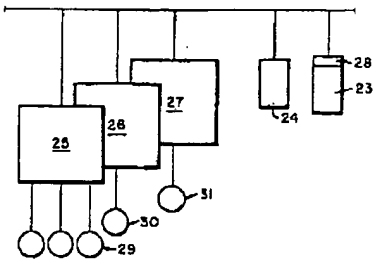
【図1】



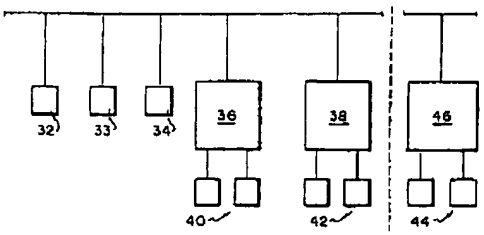
【図2】



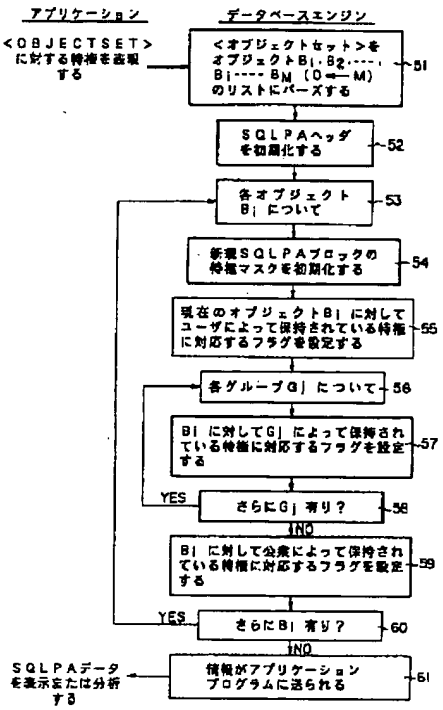
【図3】



【図4】



【図5】



【手続補正書】
【提出日】平成4年4月7日
【手続補正1】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項1】データベースのオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための方法であって、（a）所与のユーザがアクセス特権を有するオブジェクトの判定を要求する段階と、（b）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定する段階と、（c）そのユーザが間接アクセス特権を有するオブジェクトを、（1）そのユーザが属する全部のアクセスグループを自動的に判定する段階と、（2）段階（1）で判定された前記アクセスグループがアクセス特権を有するオブジェクトを自動的に判定する段階によって、自動的に判定する段階とを含むことを特徴とする方法。
【請求項2】データベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための方法であって、（a）そのユーザがその所与のオブジェクトに対してアクセス特権を有するかの判定を要求する段階と、（b）そのユーザがそのオブジェクトに対して直接アクセス特権を有するかを自動的に判定する段階と、（c）そのユーザがそのオブジェクトに対して間接アクセス特権を有するかを、
（1）そのユーザが属する全部のアクセスグループを自動的に判定する段階と、（2）段階（1）で判定されたアクセスグループの1以上がそのオブジェクトに対してアクセス特権を有するかを自動的に判定する段階によって、自動的に判定する段階とを含むことを特徴とする方法。
【請求項3】データベースのオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するためのデータベースおよび装置を含むコンピュータシステムであって、（a）所与のユーザがアクセス特権を有するオブジェクトの判定を要求するための第1の手段と、（b）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定するための第2の手段と、（c）そのユーザが間接アクセス特権を有するオブジェクトを、（1）そのユーザが属する全部のアクセスグループを自動的に判定するための第4の手段と、（2）第4の手段により判定された前記アクセスグループがアクセス特権を有するオブジェクトを自動的に判定する第5の手段とによって、自動的に判定するための第3の手段との組合せを含むことを特徴とするコンピュータシステム。

【請求項4】請求項3記載のシステムであって、前記第1の手段が、（1）アクセス特権を記述するためにコマンドを発行するための手段と、（2）記述されるオブジェクトの型を述べるための手段と、（3）記述されるオブジェクトの名称を述べるための手段と、（4）アクセス特権情報を受け取る制御ブロックの名称を述べるための手段を含むことを特徴とするシステム。

【請求項5】請求項3記載のシステムであって、さらに、（f）前記ユーザがアクセス特権を有する各オブジェクトのアクセス特権が他のユーザに拡張できるかどうかを判定するための手段と、（g）前記ユーザがアクセス特権を有する各オブジェクトのアクセス特権が他のユーザに拡張できるかどうかを表示させるための手段とを含むことを特徴とするシステム。

【請求項6】データベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するためのコンピュータシステムであって、（a）そのユーザがその所与のオブジェクトに対してアクセス特権を有するかの判定を要求するための第1の手段と、（b）そのユーザがそのオブジェクトに対して直接アクセス特権を有するかを自動的に判定するための第2の手段と、（c）そのユーザがそのオブジェクトに対して間接アクセス特権を有するかを、（1）そのユーザが属する全部のアクセスグループを自動的に判定するための第4の手段と、（2）前記第4の手段によって判定されたアクセスグループの1以上がそのオブジェクトに対してアクセス特権を有するかを自動的に判定するための第5の手段とによって、自動的に判定するための第3の手段との組合せを含むことを特徴とするシステム。

【請求項7】請求項6記載のシステムであって、前記第1の手段が、（1）アクセス特権を記述するためにコマンドを発行するための手段と、（2）その所与のオブジェクトの型を述べるための手段と、（3）そのオブジェクトの名称を述べるための手段と、（4）アクセス特権情報を受け取る制御ブロックの名称を述べるための手段とを含むことを特徴とするシステム。

【請求項8】請求項6記載のシステムであって、さらに、（d）ユーザがそのオブジェクトに対して有するアクセス特権の型を判定するための手段と、（e）前記アクセスの型を表示させるための手段とを含むことを特徴とするシステム。

【請求項9】請求項6記載のシステムであって、さらに、（f）そのオブジェクトのアクセス特権が他のユーザに拡張できるかどうかを判定するための手段と、（g）そのオブジェクトのアクセス特権が他のユーザに拡張できるかどうかを表示させるための手段とを含むことを特徴とするシステム。

【請求項10】データベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための製品であって、（a）その所与のユーザがアクセス特権を有するオブジェクトの判定を要求するための第1のプログラムコード手段と、（b）そのユーザが直接アクセス特権を有するオブジェクトを自動的に判定するための第2のプログラムコード手段と、（c）そのユーザが間接アクセス特権を有するオブジェクトを、（1）そのユーザが属する全部のアクセスグループを自動的に判定するための第4のプログラムコード手段と、（2）前記第4のプログラムコード手段により判定された前記アクセスグループがアクセス特権を有するオブジェクトを自動的に判定するための第5のプログラムコード手段とによって、自動的に判定するための第3のプログラムコード手段との組合せを含むことを特徴とする製品。

【請求項11】データベースの所与のオブジェクトに関してデータベースユーザによって現在保持されているアクセス特権を判定するための製品であって、（a）そのユーザがその所与のオブジェクトに対してアクセス特権を有するかの判定を要求するための第1のプログラムコード手段と、（b）そのユーザがそのオブジェクトに対して直接アクセス特権を有するかを自動的に判定するための第2のプログラムコード手段と、（c）そのユーザがそのオブジェクトに対して間接アクセス特権を有するかを、（1）そのユーザが属する全部のアクセスグループを自動的に判定するための第4のプログラムコード手段と、（2）前記第4のプログラムコード手段により判定されたアクセスグループの1以上がそのオブジェクトに対してアクセス特権を有するかを自動的に判定するための第5のプログラムコード手段とによって、自動的に判定するための第3のプログラムコード手段との組合せを含むことを特徴とする製品。